THE LAW SOCIETY OF IRELAND

PERSONAL DATA BREACH PROCEDURE

Version Number:	2
Date:	04 February 2019

CONTENTS

Section

Version Control and Responsibility for Maintaining the Data Protection Policy

The following people are responsible for maintaining this Data Breach Procedure

Head of F&A/Head of IT – Final Approval of all Revisions

Deirdre Byrne F&A – Providing Updates

Version Control

Version Number	Author	Purpose/Change	Date Adopted
1	F&A Department		28 September 2018
2	F&A Department	Contact details	07 February 2019

Law Society of Ireland

Personal Data Breach Procedure

What is a data breach?

A data breach is any incident which gives rise to the **unauthorised disclosure of/access to personal data processed by the Law Society** or the accidental or unlawful destruction, loss, or alteration of such data.

This may occur in a variety of contexts. Below are a few examples of how a data breach can occur within an office environment:-

- where an e mail goes to an incorrect recipient(s) (i.e. the personal data of one data subject(s) is sent erroneously to another data subject(s));
- where a letter/documents is sent to an incorrect recipient(s);
- loss/theft of a device (encrypted/unencrypted) i.e. phone/laptop/usb stick;
- loss/theft of data i.e. paper records – do you have a missing file or document?;
- where documents/data either hard or soft copy are disclosed erroneously to unauthorised individuals; and
- data being made unavailable (e.g. encrypted by malware).

How does this happen?

- Human error. Where there is a lack of attention/rushing, personal data can be disclosed erroneously.
- Inappropriate disposal of paper.
- Inadequate access controls (e.g. not locking your pc when leaving your desk, not having your laptop or phone password protected).
- Leaving confidential information in accessible areas (e.g. forgetting to remove documentation from shared photocopiers or leaving documents on a printer awaiting collection etc.)
- Curiosity getting the better of somebody.
- An in-house associate or someone from outside of the workplace tries to elicit personal data of another person that is not within their remit.
- Hacking, malware, phishing or other security attacks on IT equipment systems or networks.
- Criminal activity such as robbery - (e.g. forcing of doors, windows, items removed from filing cabinets, safes etc.).

What should I do?

- If unsure, **get help straight away**. If you suspect (but are unsure) a data breach has occurred, inform your Section/Department Head and contact the Privacy Officer immediately at Ext. 4816/dataprivacy@lawsociety.ie for guidance.

- If you know a data breach has occurred, **act immediately** and inform both your Section/Department Head and the Privacy Officer immediately. Speed is of the essence as there are regulatory rules and procedures to adhere to following a breach discovery.

- Complete the Law Society Internal Breach Form.

- Do what you can to mitigate the impact - see some tips on this at Appendix 2.

- Following risk assessment of the data breach by the Privacy Officer and IT team you will be informed of the communications to take place with the affected data subject(s).

What should I do if the breach occurs outside of business hours?

Act immediately by contacting Law Society reception on (01) 6724800 and leave your phone number and a brief detail of the issue. Reception will contact the IT team who will return your call and advise you of next steps.

What should I do if a processor or authorised person to whom I have given data advises of a breach?

If one of your processors or authorised persons makes contact with you in relation to a data breach you must act upon this reporting immediately. When a staff member becomes aware of a breach of data security (in their own area or via a Law Society data processor), he/she must report the incident to the Privacy Officer and your Section/Department Head immediately. Follow the steps at (**What should I do?).**

For example, the Law Society (the data controller) contracts an IT services firm (the data processor) to archive and store customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies us that the breach has taken in place. The Privacy Officer of the Law Society in turn notifies the DPC.

What should I not do?

- Do not ignore the issue.

- Do not delete anything – you must preserve the evidence.

- Do not choose to delay the matter. Do not keep to yourself (advise your Section/Department Head and Privacy Officer).

- Do not be afraid to ask for assistance.

In summary, it is much better to report a data protection breach straight away and the Privacy Officer will be able to advise and handle things from time of reporting. The likelihood or severity of a data breach in your area can be greatly reduced by following the guidelines as outlined in this document.

How do I know I have met my responsibilities in this regard?

Refer to the checklist at Appendix 3.

What happens next?

Information on mandatory breach notifications under GDPR

From 25th May 2018, the General Data Protection Regulation (GDPR) introduces a requirement for organisations to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals. Organisations must do this within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay.

Privacy Team and IT Team Tasks

- In the event of a breach co-operation between these two teams is key;
- Complete a Risk Assessment;
- Assess immediate needs for mitigation and damage containment (to identify the steps to be taken to mitigate the breach, such as replicating any affected data and isolating the cause of the breach);
- Assess IT remedial intervention and technical forensics required (and to appoint an external technical adviser in the matter as required);
- Assess the parties to be notified (i.e. the Data Subject(s), the Data Protection Commissioner); and
- Assess the need to advise Insurers (under Cyber Policy and Professional Indemnity Policy).

Risk assessment - what criteria does the Privacy Officer apply in the risk assessment?

Under GDPR, any data breach will need to be assessed to determine whether the mandatory breach notification obligations are triggered.

This assessment involves the Privacy Officer completing a detailed risk assessment (on a case by case basis) which will involve gathering all of the information on the breach incident taking into account all of the factors such as nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place and whether the personal data of vulnerable individuals has been exposed and then deciding on a risk rating as set out below:-

- ***Low Risk: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.***
- ***Medium Risk: The breach may have an impact on individuals but the impact is unlikely to be substantial.***
- ***High Risk: The breach may have a considerable impact on affected individuals. It includes risk that may lead to a more severe or harmful outcome for an individual than an outcome in other circumstances.***
- ***Severe Risk: The breach may have a critical, extensive or dangerous impact on affected individuals.***

In assessing risk to preserve the rights and freedoms of an individual, it is important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

> "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a data breach can have a range of adverse effects on individuals, which includes emotional distress, and physical and material damage which affects the Privacy Officer needs to identify and measure at risk assessment time.

The Privacy Officer in determining the seriousness of the data breach will consider the potential impact of the breach on individuals. In assessing this potential impact they will deliberate on the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place and whether the personal data of vulnerable individuals has been exposed. The levels of risk are further defined below:

- ***Low Risk: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.***
- ***Medium Risk: The breach may have an impact on individuals but the impact is unlikely to be substantial.***
- ***High Risk: The breach may have a considerable impact on affected individuals. It includes risk that may lead to a more severe or harmful outcome for an individual than an outcome in other circumstances.***
- ***Severe Risk: The breach may have a critical, extensive or dangerous impact on affected individuals.***

Who needs to be notified?

Notifying the Data Protection Commissioner (DPC)

The obligation to notify the DPC arises in the case of any personal data breach, unless the breach is unlikely to result in *"a risk"* to the rights and freedoms of an individual(s).

Risk categories include a broad range of physical, material and immaterial damage, such as loss of control over personal data, financial loss, identify theft and damage to reputation.

Based on this broad understanding of risk, the notification obligation, with regard to the DPC, will likely arise in a substantial number of breach events.

Even when no obligations to notify the DPC arise, the Privacy Officer will document the facts relating to the breach, its effects and any remedial action taken, in a manner that will enable the DPC to verify compliance by the Law Society with its obligations to notify the DPC in appropriate circumstances.

In summary when the risk assessment has been completed – if it is likely there will be a risk then we must notify the DPC; if it's unlikely then we do not have to report it.

You do not need to report every breach to the DPC.

Notifying data subjects

As with notifying the DPC, a risk based approach is adopted when it comes to notifying data subjects. The data subject needs to be informed about a breach if it is likely to result in a "high risk" to their rights and freedoms. This is a higher threshold than 'mere' risk in the context of notifying the DPC. One of the main reasons for this is to inform individuals the steps we have taken to lessen the effects of a data breach and so that they too can take steps to protect themselves from the effects of a breach. Any contact with those data subjects **will be made only after consultation and agreement with the Privacy Officer.** If we decide we do not need to notify individuals, the Privacy Officer will still need to notify the DPC unless we can clearly demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The DPC has authority to compel us to inform affected individuals regardless of our own decision in the matter. In any event, we document our decision-making process.

What information must we provide to individuals when telling them about a breach?

Describe, in clear and plain language, the nature of the personal data breach and, at minimum (but not obtaining the consent of your Privacy Officer so to do):

- Nature of the personal data breach and categories and approximate number of data subjects and data records concerned;
- Contact details for DPO or Organisation's point of contact;
- Likely consequences for the breach; and
- Measures to address the breach and mitigate its adverse effects for the individuals.

When to notify?

Notifications to the DPC by the Privacy Officer need to be made without undue delay, and if not made within 72 hours of the Privacy Officer becoming aware of the issue, the Privacy Officer will need to explain any delay. Furthermore, where it is not possible to provide all relevant information at once, it may be provided in phases, again without undue further delay. This means the Privacy Officer must consider notifying breaches before we have been able to carry out a full risk assessment, failing which we need to explain the delay to the DPC.

Notifications to the Data Subject need to be made without undue delay but without the 72 hour proviso. However, there are some circumstances in which no notification to individuals will be required, such as where the data has been encrypted, or steps have been taken to ensure that the high risk is no longer likely to materialise.

See Appendix 4: Flowchart showing notification requirements

Appendix 1
DATA BREACH REPORT FORM

If you discover a data breach, please notify your Section/Department Head and contact the Privacy Officer immediately at Ext. 4816/dataprivacy@lawsociety.ie. Please complete this form and return it to the Privacy Officer at **dataprivacy@lawsociety.ie within 24 hours** of becoming aware of the breach.

Notification of Personal Data Breach

Name of person reporting incident:	
Contact details of person reporting incident:	
Date(s)/time of Breach(s):	
Date/time Incident was discovered:	
Type of Data Breach: e.g. lost/stolen device, network security compromise, lost/stolen paper:	
Names of data subject(s) affected and Society relationship:	
Data compromised by Breach. (Personal/Special Category etc.). Please attach a copy of the data:	
Description of Data Breach (e.g. cause, what else?	
Number of Data Subjects affected – if known:	
Description of any action(s) since breach was discovered:	
For Finance and Administration Unit use only	
Report received by:	
Date/time:	
Actions taken and dates:	
Assessment Re: advising Data Subject:	
Date of report to DPC and follow actions:	
Debrief with staff report to Department Head:	

Appendix 2
Steps to mitigate a data breach

- When drafting or writing an email take out your recipient listing. Put it in the body of your email. The very last thing you should do is put in the recipients listing to avoid any mistakes.

- When sending a communication using several recipients externally the “Bcc” (blind copy) field should be used to prevent the unnecessary disclosure of recipients’ email addresses.

- Check and recheck your email address is correct before pressing send (use the four eyes approach and ask a colleague to double check your work).

- Our email system automatically tells us when a mail is going externally to the Organisation, be extra careful in these checks that you have the correct email address.

- Check you have no additional attachments, third party data or sensitive personal data that should not be included.

- When sending data in the post or DX double check you have the correct address.

- Do not send Card number, Pin or any other credit card information to anyone by email or a scanned document attached to an email.

- Keep your work area tidy and treat all personal data as you would like your data to be treated.

- Read the Top Tips documents on the Intranet (Data Protection Centre) such as message recall.

Appendix 3
Checklist

Staff Member notifying a personal data breach to Privacy Officer:

☐ I have recognised a personal data breach and notified my Section/Department Head and telephoned and emailed the Privacy Officer.

☐ I have contacted Law Society Head office number as my incident occurred out of business hours.

☐ I have not deleted any of the relevant documents related to this data breach.

☐ I have completed the internal data breach report form and enclosed relevant documents.

☐ I have completed and documented the steps that I have taken to mitigate this matter.

☐ I have made contact with the affected data subjects (where this is required) with guidance from the Privacy Officer.

Appendix 4
Flowchart of notification requirements